(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
28 juillet 2005 (28.07.2005)

PCT

(10) Numéro de publication internationale
WO 2005/069658 A1

(51) Classification internationale des brevets[7] : H04Q 7/32

(21) Numéro de la demande internationale :
PCT/EP2004/053469

(22) Date de dépôt international :
14 décembre 2004 (14.12.2004)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
03/15078 19 décembre 2003 (19.12.2003) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **GEMPLUS** [FR/FR]; Avenue du Pic de Bertagne, Parc d'activité de Gémenos, F-13420 Gémenos (FR).

(72) Inventeurs; et

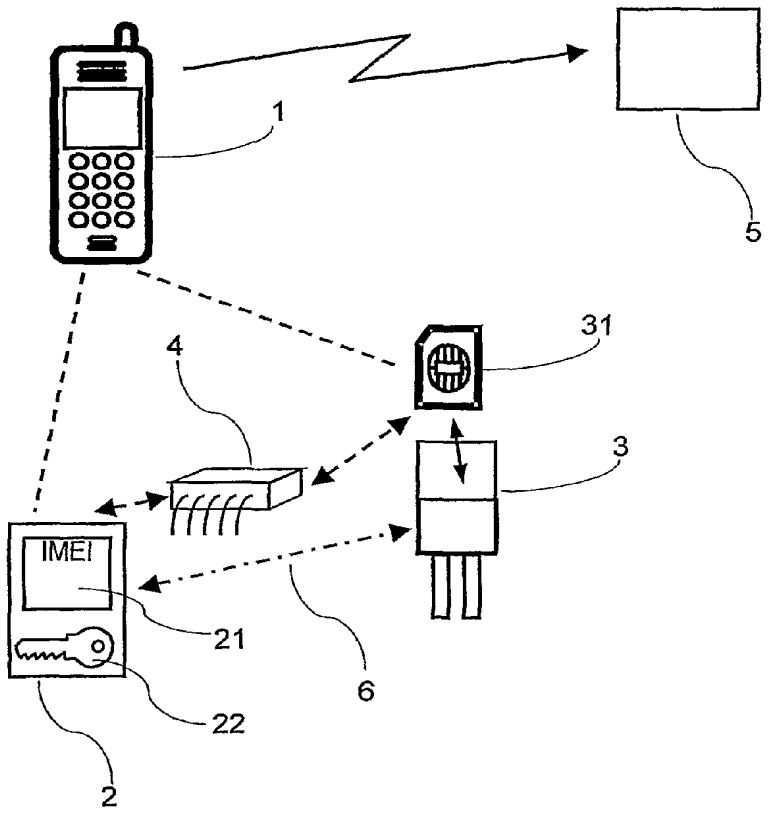
(75) Inventeurs/Déposants *(pour US seulement)* : **BOURSIER, Carine** [FR/FR]; 38, chemin de St Michel, F-13400 Aubagne (FR). **GIRARD, Pierre** [FR/FR]; 942, chemin du Tourtaret, F-13112 La Destrousse (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB,

[Suite sur la page suivante]

(54) Title: METHOD OF SECURING A MOBILE TELEPHONE IDENTIFIER AND CORRESPONDING MOBILE TELEPHONE

(54) Titre : PROCEDE DE SECURISATION DE L'IDENTIFIANT D'UN TELEPHONE PORTABLE, ET TELEPHONE PORTABLE CORRESPONDANT



(57) Abstract: The invention relates to a mobile telephone handset (1) comprising: a storage support (2) which is secured against fraudulent access and which stores the IMEI (21) of the handset; a connector (3) for a secure electronic module (31) which is associated with an operator; and a handset (1) operating system (4) which controls (i) authentication of the IMEI storage support (2) by a secure electronic module which is connected to the aforementioned connector in order to establish a secure communication channel (6) between the storage support and the module and (ii) transmission of the IMEI over the secure channel to the secure electronic module. The invention also relates to an associated method. The invention can be used to prevent the dynamic modification of the IMEI during the transmission thereof.

[Suite sur la page suivante]

WO 2005/069658 A1

GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* **:** ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : L'invention propose un combiné de téléphonie mobile (1), comprenant: un support de stockage (2) sécurisé contre les accès frauduleux, stockant l'IMEI (21) du combiné; un connecteur (3) d'un module électronique sécurisé (31) associé à un opérateur; un système d'exploitation (4) du combiné (1), commandant l'authentification du support de stockage (2) de l'IMEI par un module électronique securisé connecté au connecteur afin d'établir un canal de communication sécurisé (6) entre le support de stockage et le module, et commandant la transmission de l'IMEI sur le canal sécurisé vers le module électronique sécurise. L'invention concerne également un procédé associé. L'invention permet notamment d'empêcher la modification dynamique de l'IMEI lors de sa transmission.

PROCÉDÉ DE SÉCURISATION DE L'IDENTIFIANT D'UN TÉLÉPHONE PORTABLE, ET TÉLÉPHONE PORTABLE CORRESPONDANT

La présente invention porte sur les combinés de téléphonie mobile, et plus particulièrement sur les techniques visant à réduire les possibilités de réutilisation d'un combiné volé.

Le vol de combinés de téléphonie portable est devenu un véritable problème de société. Les vols avec violence dans les lieux publics ont ainsi massivement augmenté ces dernières années du fait des vols de tels combinés. On peut par exemple estimer que le nombre de téléphones portables volés en France durant l'année 2001 a été supérieur à 150 000. Pour combattre ces vols, les autorités françaises obligent dorénavant les opérateurs de téléphonie mobile à placer un identifiant des combinés volés sur une liste noire. Chaque combiné mobile présente une identification unique appelée IMEI (pour International Mobile Equipment Identity en langue anglaise) qui est transmise au réseau utilisé pour la communication. L'IMEI d'un combiné déclaré volé est ainsi placée dans une liste noire, qui est déjà opérationnelle en France. Lorsqu'un combiné inscrit dans la liste tente de communiquer, ses communications peuvent être bloquées.

Cependant, l'IMEI est actuellement stockée sur une mémoire flash et mal sécurisée. En effet, des logiciels permettent de modifier l'IMEI d'un combiné et sont disponibles en masse sur internet. Ainsi, comme cela a été reconnu par la Commission Européenne, la mise en

place de listes noires de combinés volés peut être contournée relativement aisément.

Une recommandation technique de l'ETSI propose de rendre l'IMEI inchangeable après le processus de fabrication du combiné. Cette recommandation a notamment été mise en œuvre en inscrivant l'IMEI dans une PROM, afin qu'elle ne puisse pas physiquement être modifiée.

Cette technique de sécurisation présente des inconvénients. En effet, l'IMEI est lue par le système d'exploitation du combiné. L'utilisation de systèmes d'exploitation frauduleux permet ainsi de modifier l'IMEI de façon logicielle afin de fournir une IMEI modifiée au réseau.

L'invention vise à résoudre ces inconvénients. L'invention a ainsi pour objet un combiné de téléphonie mobile comprenant :

-un support de stockage sécurisé contre les accès frauduleux, stockant l'IMEI du combiné ;

-un connecteur d'un module électronique sécurisé associé à un opérateur;

-un système d'exploitation du combiné, commandant l'authentification du support de stockage de l'IMEI par un module électronique sécurisé connecté au connecteur afin d'établir un canal de communication sécurisé entre le support de stockage et le module, et commandant la transmission de l'IMEI sur le canal sécurisé vers le module électronique sécurisé.

Selon une variante, le système d'exploitation commande la transmission de l'IMEI à un opérateur de

téléphonie mobile par l'intermédiaire d'un canal sécurisé OTA.

Selon une autre variante, le combiné comprend un module électronique sécurisé associé à l'opérateur connecté dans le connecteur. Selon encore une variante, le module électronique sécurisé est une carte UICC.

On peut alors prévoir que le système d'exploitation commande l'authentification du module sécurisé par le support de stockage.

Selon une variante, le module électronique sécurisé et le support de stockage stockent des clés de cryptage adaptées pour sécuriser le canal de communication sécurisé.

Selon une autre variante, le module sécurisé bloque l'utilisation du combiné lors de la détection d'une IMEI falsifiée.

L'invention porte également sur un procédé de sécurisation de l'IMEI d'un combiné de téléphonie mobile, comprenant les étapes :

-d'authentification d'un support de stockage sécurisé du combiné mémorisant son IMEI, par un module électronique sécurisé associé à l'opérateur et inséré dans un connecteur du combiné, afin d'établir un canal sécurisé entre le support de stockage et le module sécurisé;

-de transmission de l'IMEI depuis le support de stockage jusqu'au module sécurisé par l'intermédiaire du canal sécurisé.

Selon une variante, le module sécurisé transmet en outre l'IMEI à un opérateur de téléphonie mobile par l'intermédiaire d'un canal sécurisé OTA.

Selon encore une variante, l'opérateur compare l'IMEI à une liste noire de combinés volés, et bloque les communications du combiné lorsque le combiné appartient à la liste noire.

Selon une autre variante, le module sécurisé bloque l'utilisation du combiné lors de la détection d'une IMEI falsifiée.

D'autres particularités et avantages de l'invention apparaîtront clairement à la lecture de la description faite à titre d'exemple non limitatif et en regard des dessins annexés sur lesquels :

-la figure 1 représente des éléments mis en œuvre selon une variante de l'invention ;

-la figure 2 représente un diagramme illustrant les échanges et étapes réalisés par des éléments selon une variante de l'invention .

L'invention propose d'utiliser un canal sécurisé afin de réaliser une authentification d'un support de stockage (sécurisé contre les accès frauduleux et mémorisant l'IMEI) par un module électronique sécurisé associé à l'opérateur et connecté dans le combiné mobile. Un tel module électronique sécurisé se présente typiquement sous la forme d'une carte UICC (pour Universal Integrated Circuit Card en langue anglaise) par exemple au format d'une carte SIM. L'IMEI n'est transmise sur le canal sécurisé que lorsque le support de stockage de l'IMEI a été authentifié.

La figure 1 illustre ainsi un combiné de téléphonie mobile 1 selon l'invention. Le combiné 1 comprend un

support de stockage 2 sécurisé contre les accès frauduleux. Ce support de stockage 2 stocke l'IMEI 21 du combiné 1. Le combiné 1 comprend en outre un connecteur 3 pour un module électronique sécurisé tel qu'une carte UICC 31. Un canal de communication sécurisé 6 est établi entre le module électronique sécurisé 31 connecté dans le connecteur 3 et le support de stockage sécurisé 2. Le canal de communication sécurisé 6 signifie qu'au moins le module sécurisé authentifie le support de stockage 2 par tout moyen approprié et garantit l'intégrité et la confidentialité de toutes les données échangées. Un système d'exploitation 4 du combiné, commande l'authentification du support de stockage 2 de l'IMEI 21 par le module sécurisé 31 connecté dans le connecteur (identifié par l'étape 101 à la figure 2), et commande la transmission de l'IMEI sur le canal sécurisé 6 vers ce module sécurisé 31 (identifié par l'étape 102 à la figure 2).

L'IMEI est ainsi sécurisée contre les modifications dynamiques lors de sa transmission sur le canal de communication 6. On peut donc considérer que l'IMEI reçue par le module 31 est authentifiée car elle provient du support de stockage authentifié 2 et a été transmise par l'intermédiaire du canal de communication sécurisé 6.

Bien entendu, si l'authentification du support de stockage 2 de l'IMEI par le module électronique sécurisé 31 signale une erreur, ce module électronique

31 peut prendre toute mesure adaptée pour signaler cette erreur ou empêcher l'utilisation du combiné.

On peut ainsi bloquer le combiné sans avoir recours à une communication avec le réseau de l'opérateur. L'opérateur peut notamment éviter d'avoir à gérer les clés ou les certificats associés à un combiné. Un tel blocage est donc plus facile à mettre en œuvre. Un tel blocage du téléphone peut également être réalisé sans nécessiter de modifications des réseaux des opérateurs : les infrastructures et protocoles du réseau existant peuvent ainsi être conservés.

Le support de stockage 2 sécurisé contre les accès frauduleux peut être d'un type connu, par exemple une PROM. L'intégrité statique de l'information qui y est inscrite est ainsi assurée.

Afin de sécuriser le canal 6 et de réaliser toute authentification voulue entre le support de stockage 2 et le module 31, le support 2 et/ou le module peuvent stocker des clés de cryptage adaptées au type de cryptage ou d'authentification souhaités. Des types de cryptage ou d'authentification utilisables sont connus en soi. On peut notamment prévoir d'utiliser des clés de session ou des clés statiques.

L'intégrité de l'IMEI peut être protégée par un calcul cryptographique qui serait transmis sur le canal sécurisé 6 au module sécurisé 31.

Le système d'exploitation 4 peut être mémorisé dans une mémoire ROM et exécuté par un microcontrôleur. Le

système d'exploitation 4 établira de préférence un canal sécurisé entre le support 2 et le module sécurisé 31 au moment de l'initialisation du combiné de téléphonie, ou en préalable à un appel.

Le système d'exploitation 4 peut être configuré pour que le module sécurisé 31 authentifie le combiné et vérifie l'intégrité des données qui lui sont transmises. On peut également prévoir que le module sécurisé 31 soit authentifié par le support sécurisé 2 du mobile 1 et vérifie également l'intégrité des données qui lui sont transmises.

On peut également prévoir des moyens de calcul cryptographiques intégrés dans le module sécurisé 31.

L'utilisation des listes noires doit malgré tout être poursuivie pour prendre des mesures de blocage. L'IMEI peut notamment être transmise du module sécurisé vers le réseau de l'opérateur, éventuellement en utilisant un canal sécurisé entre le module sécurisé 31 et l'opérateur ou afin de comparer l'IMEI authentifiée à une liste noire et éventuellement obtenir une commande de blocage du combiné de la part du réseau. Dans l'exemple de la figure 2, l'IMEI est transmise à un serveur 7 à l'étape 103. Le serveur établit si cet IMEI est présente dans sa liste noire. A l'étape 104, le serveur transmet au combiné une indication de la présence ou non de l'IMEI dans la liste. Une indication de présence d'une IMEI dans la liste peut correspondre à une commande de blocage du combiné par le serveur. Le serveur peut bien entendu prendre toute autre mesure adéquate pour perturber l'utilisateur frauduleux. Le

serveur peut notamment déconnecter le combiné du réseau de communication de l'opérateur ou commander au module sécurisé de cesser la génération de clés pour le combiné.

Plusieurs modes de transmission de l'IMEI peuvent être envisagés entre le module sécurisé et le réseau de l'opérateur.

Cette transmission peut notamment être effectuée par l'intermédiaire du réseau de communication de l'opérateur, destiné à transmettre les communications entre utilisateurs. Dans l'exemple de la figure 1, la transmission est effectuée entre le combiné et un opérateur 5 d'un réseau de communication.

La transmission s'effectuera plutôt par l'intermédiaire d'un canal sécurisé, afin d'accroître le niveau de sécurité de la transmission. On peut notamment utiliser le canal sécurisé OTA initialement destiné à transmettre des SMS sécurisés et notamment utilisé pour le transfert d'applets, vers le module sécurisé.

REVENDICATIONS

1. Combiné de téléphonie mobile (1), caractérisé en ce qu'il comprend :
   -un support de stockage (2) sécurisé contre les accès frauduleux, stockant l'identification IMEI (21) du combiné ;
   -un connecteur (3) d'un module électronique sécurisé (31) associé à un opérateur;
   -un système d'exploitation (4) du combiné (1), commandant l'authentification du support de stockage (2) de l'IMEI par un module électronique sécurisé connecté au connecteur afin d'établir un canal de communication sécurisé (6) entre le support de stockage et le module, et commandant la transmission de l'IMEI sur le canal sécurisé vers le module électronique sécurisé.

2. Combiné de téléphonie mobile (1) selon la revendication 1, caractérisé en ce que le système d'exploitation (4) commande la transmission de l'IMEI à un opérateur de téléphonie mobile (5) par l'intermédiaire d'un canal sécurisé OTA.

3. Combiné selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend un module électronique (31)

sécurisé associé à l'opérateur connecté dans le connecteur.

4. Combiné selon la revendication 3, caractérisé en ce que le module électronique sécurisé est une carte UICC.

5. Combiné selon la revendication 3 ou 4, caractérisé en ce que le système d'exploitation commande l'authentification du module sécurisé par le support de stockage.

6. Combiné selon la revendication 5, caractérisé en ce que le module électronique sécurisé et le support de stockage stockent des clés de cryptage (22) adaptées pour sécuriser le canal de communication sécurisé (6).

7. Combiné selon l'une quelconque des revendications 3 à 6, caractérisé en ce que le module sécurisé (31) bloque l'utilisation du combiné lors de la détection d'une IMEI falsifiée.

8. Procédé de sécurisation de l'identification IMEI d'un combiné de téléphonie mobile (1), comprenant les étapes ;

-d'authentification d'un support de stockage sécurisé du combiné mémorisant son IMEI (21), par un module électronique sécurisé (31) associé à l'opérateur et

inséré dans un connecteur (3) du combiné, afin d'établir un canal sécurisé entre le support de stockage et le module sécurisé;

-de transmission de l'IMEI (21) depuis le support de stockage jusqu'au module sécurisé par l'intermédiaire du canal sécurisé.

9. Procédé selon la revendication 8, caractérisé en ce que le module sécurisé (31) transmet en outre l'IMEI à un opérateur de téléphonie mobile par l'intermédiaire d'un canal sécurisé OTA.

10. Procédé selon la revendication 9, caractérisé en ce que l'opérateur compare l'IMEI à une liste noire (7) de combinés volés, et bloque les communications du combiné lorsque le combiné appartient à la liste noire.

11. Procédé selon l'une quelconque des revendications 8 à 10, caractérisé en ce que le module sécurisé bloque l'utilisation du combiné lors de la détection d'une IMEI falsifiée.

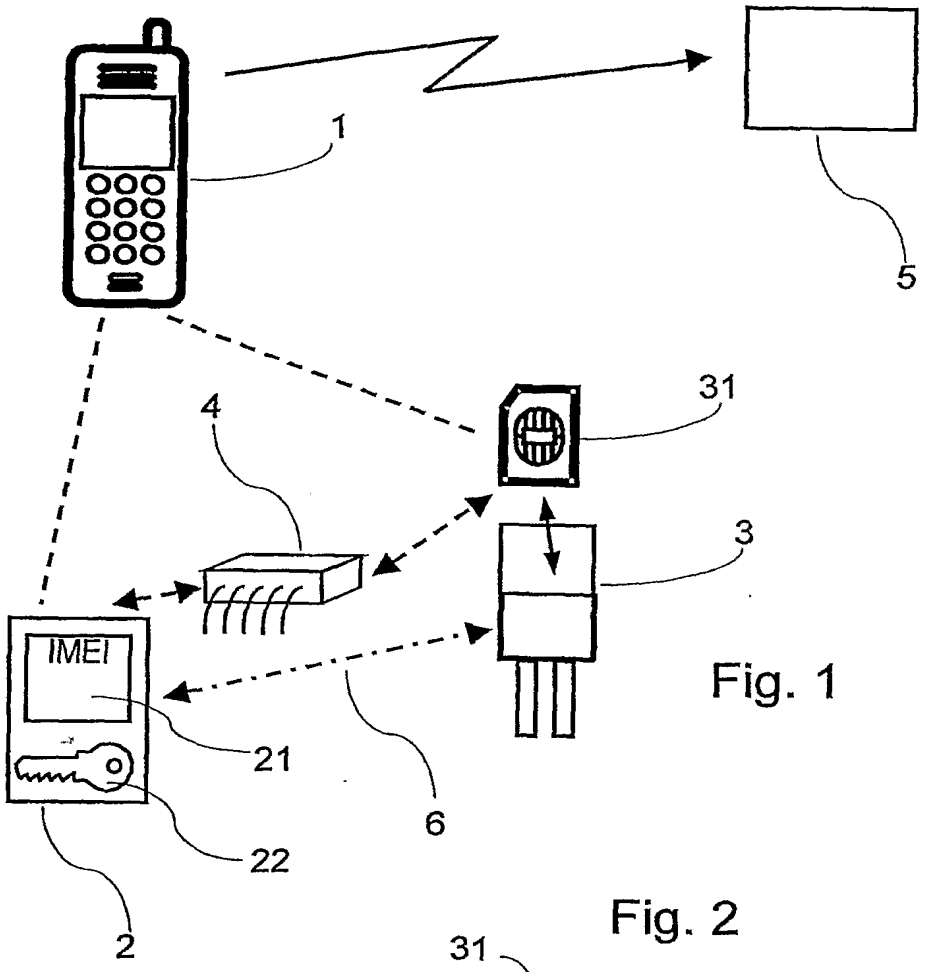
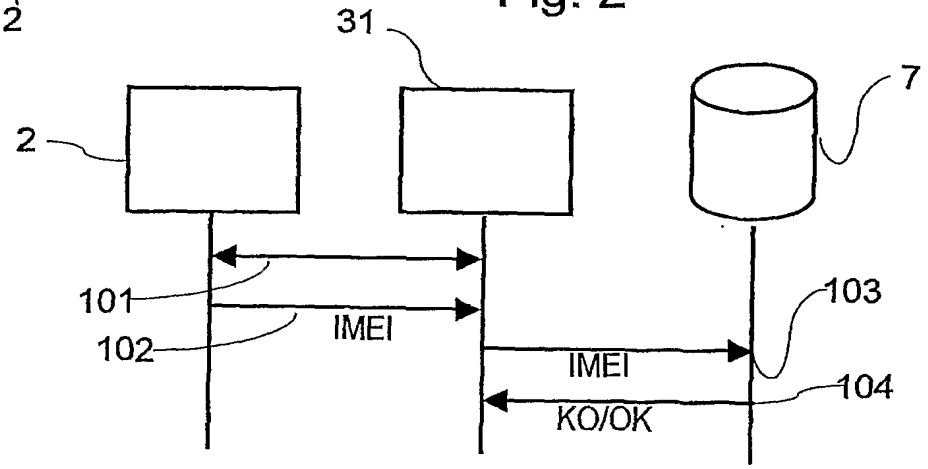


Fig. 1

Fig. 2



INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/053469

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04Q7/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04Q G07F G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE 100 26 326 A (BOSCH GMBH ROBERT) 29 November 2001 (2001-11-29) paragraphs '0008!, '0009!, '0014!, '0054!, '0061!, '0062!, '0067!, '0075! claims 1,13	1-11
A	FR 2 797 138 A (SAGEM) 2 February 2001 (2001-02-02) page 2, line 13 - page 3, line 6 page 7, line 31 - page 8, line 12	1-11

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 March 2005	07/04/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Kampouris, A

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/053469

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 10026326 A	29-11-2001	DE 10026326 A1	29-11-2001
		WO 0191478 A2	29-11-2001
		EP 1290905 A2	12-03-2003
		JP 2003535497 T	25-11-2003
		US 2004111616 A1	10-06-2004
FR 2797138 A	02-02-2001	FR 2797138 A1	02-02-2001
		DE 10036414 A1	08-03-2001
		GB 2355892 A ,B	02-05-2001

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/EP2004/053469

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04Q7/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04Q G07F G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	DE 100 26 326 A (BOSCH GMBH ROBERT) 29 novembre 2001 (2001-11-29) alinéas '0008!, '0009!, '0014!, '0054!, '0061!, '0062!, '0067!, '0075! revendications 1,13	1-11
A	FR 2 797 138 A (SAGEM) 2 février 2001 (2001-02-02) page 2, ligne 13 - page 3, ligne 6 page 7, ligne 31 - page 8, ligne 12	1-11

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée
"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
23 mars 2005	07/04/2005

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Kampouris, A

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/EP2004/053469

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
DE 10026326 A	29-11-2001	DE 10026326 A1	29-11-2001
		WO 0191478 A2	29-11-2001
		EP 1290905 A2	12-03-2003
		JP 2003535497 T	25-11-2003
		US 2004111616 A1	10-06-2004
FR 2797138 A	02-02-2001	FR 2797138 A1	02-02-2001
		DE 10036414 A1	08-03-2001
		GB 2355892 A ,B	02-05-2001